In the Claims

1. (currently amended) A method for use in the monitoring of communications traffic, comprising the step of recording the ~~said~~ traffic and storing the recorded traffic ~~in an~~ as encrypted data ~~format~~ such that the data can be decrypted only by means of keys that exhibit restricted availability.

2. (currently amended) A method as claimed in Claim 1 ~~and arranged to employ~~ further including employment of a spare disk and/or CPU capacity within a telecommunications system.

3. (currently amended) A method as claimed in Claim 1 ~~or 2 and~~ further including the step of including encrypted search conditions within the decryption keys that are made selectively available.

4. (currently amended) A method as claimed in Claim 1, ~~2 or 3, and~~ further including the step of employing separate levels of ~~authorisation~~ authorization for access to the stored data.

5. (currently amended) A method as claimed in ~~any one or more Claims 1-4, and~~ Claim 1, further including the step of employing a decryption key that is useable only once.

6. (currently amended) A method as claimed in Claim 1, further ~~any one or more of the preceding claims, and~~ including the step of logging all accesses to the stored data to an encrypted secure audit trail.

7. (currently amended) A method as claimed in Claim 1, further ~~any one or more of the preceding claims and~~ including a tamper detection reference within the encrypted data.

8. (currently amended) A method as claimed in Claim 1, further ~~any one or more of the preceding claims, and~~ including the step of monitoring all the available communications traffic.

9. (currently amended) A method as claimed in Claim 8, wherein ~~and when~~ the step of storing the recorded traffic comprises the step of recording all of the recorded traffic.

10. (currently amended) A method as claimed in Claim 1, ~~any one or more of the preceding claims,~~ wherein the communications traffic to be recorded comprises traffic through a telecommunications switch, router or gateway.

11. (currently amended) A method as claimed in Claim 1, further ~~any one or more of the preceding claims, and~~ including the step of encrypting details relating to the communications traffic and storing the said encrypted details for subsequent access.

12. (currently amended) A method as claimed in Claim 1, further ~~any one or more of the preceding claims and~~ including the step of ~~authorising~~ authorizing use of the required decryption key in a restricted manner.

13. (currently amended) A system for use in the monitoring of communications traffic, comprising in combination:

~~including means for recording~~ a recorder that records the ~~said~~ traffic, and

~~means for storing~~ a storage device that stores the recorded traffic as encrypted data, such that the recorded data can be decrypted only by means of keys that exhibit restricted availability.

14. (currently amended) A system as claimed in Claim 13 further including application software ~~and arranged with means for executing~~ that executes the method steps of any one or more of Claims 2-12.

15. (currently cancelled) A method for use in the monitoring of telecommunications traffic substantially as hereinbefore described with reference to, and as illustrated in the accompanying drawing.

16. (currently cancelled) A system for use in the monitoring of telecommunications traffic substantially as hereinbefore described with reference to, and as illustrated in the accompanying drawing.

17. (new) A method for use in the monitoring of communications traffic, comprising the steps of:

recording the traffic;

storing the recorded traffic as encrypted data such that the data can be decrypted by decryption keys that exhibit restricted availability, that allow encrypted search conditions and that employs separate levels of authorization for access to the stored data; and

encrypting details relating to the communications traffic and storing the said encrypted details for subsequent access.

18. (new) The method as claimed in Claim 17, further including the step of employing a decryption key that is useable only once.

19. (new) The method as claimed in Claim 17, further including the step of logging all accesses to the stored data to an encrypted secure audit trail.

20. (new) The method as claimed in Claim 17, further including a tamper detection reference within the encrypted data.

21. (new) The method as claimed in Claim 17, further including the step of monitoring all the available communications traffic.

22. (new) The method as claimed in Claim 17, wherein the step of storing the recorded traffic comprises the step of recording all of the recorded traffic.